E - Security

Mridul Pal*

1. Introduction

Almost everyday we hear that the system run by the government and private organizations have been penetrated or hacked. Even U.S. Military system and Microsoft organization have been hacked or defaced. As we become increasingly reliant upon information technology and communication technology, the exploitation by cyber-criminals poses an ever-greater threat to the public infrastructure. Criminals are targeting computers and telecommunication systems to obtain or alter valuable information and sometimes they attempt to disrupt critical public and commercial safety. Even the criminals including the members of organized crime groups and terrorists are using technologies to facilitate traditional offences. So, as a whole, the misuse of information system has become a serious threat to us.

Most commonly adopted security technology in the industries are Anti-virus (91%), Instrusion Detection System (38%), Security Gateways like login /password (68%) and firewall (39%). But unfortunately, only 20% of the corporate sectors consider this security issue extremely important and about 74% understand that it is somewhat important. Statistics says that about 76% attacks are from virus/Trojan/worm and 13% are attacked by unauthorized access.

The only way to thoroughly protect a system is through a layered strategy commonly referred to as Defense in Depth. This solution often addresses the following primary areas of security

1. Perimeter Defenses like border routers and firewalls.
2. Network Defenses such as an Intrusion Detection System
3. Application Protection
4. Virus Detection
5. Encryption
6. Policy Definition and Management.
7. Monitoring

2. Common Network Attacks

Hackers : Hackers are persons that gain unauthorized access to computer resources to steal valuable data or sabotage systems. These hackers are not professional cyber terrorists, they use programs to cause malicious damage such as defacing of web sites.

Physical break-ins and theft : Security attacks don't only happen over the internet. There is still the old fashioned route : physical access to the hardware and software. All the firewalls, virus scanners and encryption measures will not be able to protect a system if a malicious individual gains unauthorized, physical access to the system and destroys or steals computer equipment, including valuable data within it. The situation gets a little more critical if the machine is set up to access the corporate networks via a remote dial-up or virtual private network connection in which the password mechanism can be easily defected by the password cracking tools available on the internet.

Insiders : Sometimes the insiders like current employees and former workers represent the most dangerous security threats since they know how the computer systems work and more importantly, they have authorized access to network resources and critical information.

Denial-of-Service attacks : In a DOS attack, Web-servers and networks are flooded with sudden and overwhelming bursts of network

*Technical Assistant, Computer Science & Engineering

data, slowing down server performance and eventually erasing the website. This can cause severe damage to databases but a DOS attack only interrupts network service for a limited period.

E-commerce not secure : Recent survey shows that while the security of credit card numbers and personal information are the most important security concerns of customers, less than 35% of organizations perform security audits on e-commerce system.

Virus & Worms : These attacks are the most common form of security breaches.

3. Ways to Combat the E-security Challenges

To combat the e-security challenges, several processes are in use such as

1. Firewalls
2. Intrusion Detection System
3. Biometric
4. Digital Signature.

3.1 Firewalls

Firewalls are the first line of defense against attackers from the outside world. A firewall acts as a sentry between the Internet and the local internal network. Today, firewalls are more critical since internet based attacks on Web-servers are on the rise.

3.2 Intrusion Detection System

Intrusion Detection System is the ongoing process of searching for security violations on the networks. This system includes protective and reactive detection of vulnerabilities, analysis and corresponding responses. Actually there exists a lot of services to investigate the intrusion at the network. Among these the poor network perimeter signifies the access to the devices across the network without having any access control using firewall or packet filtering router, not to scan the TCP/UDP port and scanning logon accounts. Besides, shared networks are easier to get attacked as all traffic is visible from everywhere on that shared media. Poor physical security includes the bypassing security routers, switches, password cracking etc. One solution to tackle such unwanted intruders is from CISCO's IOS intrusion Detection System which is integrated into the router IOS. Any traffic that passes through the router can be scrutinized for intrusion.

3.3 Biometrics

The measurement of one or more physical or behavioral characteristics of an individual is used to increase the security level without increasing the complexity. Biometric identifiers are highly reliable since they cannot be easily faked or altered. Biometric can also be employed to verify the identification with a high level of accuracy by incorporating them directly into *security devices. Biometric technologies are* defined as "automated methods of identifying or authorising the identity of a living person based on a physiological or behavioral characteristics". A physiological characteristic is a relatively stable physical characteristic such as fingerprints, eye patterns, facial features, hand geometry (although general physical traits, such as size and sex have a major influence). Behavioral identifiers include voice print, signatures, keystrokes etc. But they can vary because of external conditions such as illness.

Biometric system consists of the following components :

1. A device or sensor that measures the characteristic.
2. An algorithm that processes the signal and compares it with a standardized representation of the individual's biometric feature.
3. A decision module that determines whether the comparison is acceptable and passes the result to the application.
4. A management framework and supporting processes.

The biometric system actually captures the data set of the single user, processes it to remove

noise and extracts key determining features for comparison with the entire database of templates. The template that corresponds most closely to the feature set of subjects is deemed to identify the subject.

3.4 Digital Authentication & Digital Signature

Digital authentication systems are expected to become an essential part of doing business via the internet. *Authentication* is any process through which one proves and verifies certain information. Sometimes one may want to verify the origin of a document, the identity of the sender, the time and date of sending a document, the identity of a computer or user, and so on. A *digital signature* is a cryptographic mean through which many of these may be verified. Based on a range of encryption techniques, digital signature systems allow people and organizations to electronically certify such features as their identity, their ability to pay, or the authenticity of an electronic document.

Besides, PKI (Public Key Infrastructure) is a very well accepted software programming implementation way to cipher a text message over the net. And also, there are many ways to protect a PC to ensure desktop security. This type of security measure is inherent within the particular operating system like Windows-NT and different Unix Brands.

4. Secure E-banking Services

Banks need to look after every opportunity to meet the customer needs. When a company provides an online service, it means that the organization is exposing itself to the public. Opening up the organizations's network can lead to exploitation by hackers. To be successful, banks need to take necessary precautions to overcome the risk. Data protection and prevention of any vulnerability are crucial to the bank's operation. The security assessment/ethical hacking reviews the overall network infrastructure of the bank, simulates unauthorized access activities into the bank web-server to look for vulnerabilities and come up with recommendations for any weakness found. The managed security service provides a real-time intrusion detection system that intelligently analyzes network activity to detect any actual or attempted intrusion into the network. The powers of an advanced intrusion detection engine and an intelligent firewall is a combined in a desktop protector which is a revolutionary new way to detect, monitor and block intrusion.

5. Conclusion

Finally to tackle the challenges of the information age, the government has formed a inter-departmental working group on computer related crime to review and make suggestions to strengthen the framework of law enforcement against such crime. Also this type of government effort must be complemented by a new level of support from the community. Though it is an obvious fact that no single system can be made 100% secure but the use of authentication devices for securing small office/home office computing, information openness and data integrity can increase the effectiveness of what we desire about security.

"Concern for man himself and his fate must always be the chief interest of all technical endeavours in order that the evolution of our mind shall be a blessing and not a curse to mankind. Never forget this in the midst of your diagrams and equations."

– Albert Einstein